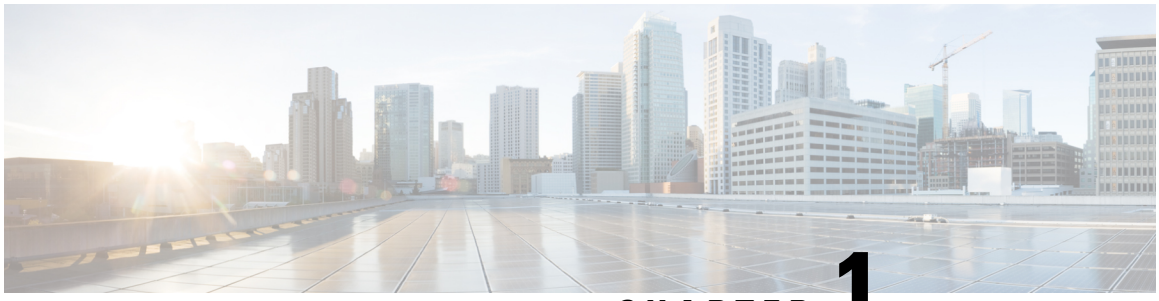
Cisco LoRaWAN Pluggable Interface Module Installation and Configuration Guide

First Published: 2022-08-04

Last Modified: 2023-01-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Installing the P-LPWA-XXX Pluggable Module

This chapter contains the following sections:

Cisco LoRaWAN Pluggable Module Overview

LoRa®

LoRa® is a low power wide area network (LPWAN) RF physical layer modulation technology that offers long-distance wireless connectivity, excellent power efficiency, very high receiver sensitivity, and robust spectrum spreading. It operates on unlicensed Industrial, Scientific, and Medical (ISM) frequencies, for which 863 - 870 MHz spectrum and spectrum subsets are available for Europe, the Middle East, Africa, and India, and 902 - 928 MHz spectrum and spectrum subsets can be utilized in the Americas and in Asia-Pacific countries.

LoRa Alliance®

Wide Area networks for the Internet of Things. Launched at Mobile World Congress in 2015, the LoRa Alliance® is an open, non-profit association of Members that are developing and deploying Internet of Things (IoT) solutions now.

LoRaWAN®

LoRaWAN® is a MAC (Media Access Control) protocol specification defined by the LoRa Alliance that complements the LoRa® physical layer. It is supported by an established ecosystem of LoRaWAN compliant

devices that are available from multiple vendors, and which can be certified for interoperability by the LoRa Alliance.

The Cisco LoRaWAN Pluggable Interface Module

The Cisco LoRaWAN Pluggable Interface Module supports eight channels of LoRa connectivity.

There are two different P-LPWA modules:

- The P-LPWA-900 is designed for RF regional profile US915, AS923 and AU915 as defined by the LoRa Alliance RF regional profile specifications.
- The P-LPWA-800 is designed for the EU868, IND865 and RU864 RF regional profile as defined by the LoRa Alliance RF regional profile specifications.

The Cisco LoRaWAN pluggable modules can be managed by command line interface (CLI), or the Cisco IOS XE Web User Interface (WebUI).

The following figure shows the P-LPWA-900.

Figure 1: P-LPWA-900 LoRaWAN Pluggable Interface Module

The following figure provides details for the Cisco LoRaWAN pluggable module:

Figure 2: Module Details

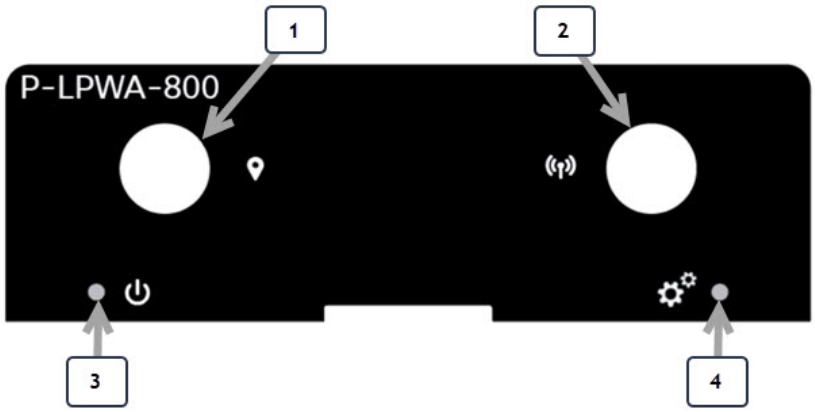


Table 1: Module Details

Item	Description
1	GNSS Connector SMA(f)
2	LoRa RF Connector SMA(f)
3	LoRa Power LED
4	LoRa Status LED

The module dimensions are 2.50” x 0.85” x 3.30” (6.35cm x 2.16cm x 8.38cm). The module weighs 0.4 lbs (181.4 grams).

Note Additional information can be found in the Cisco LoRa WAN Deployment Guide.

Guidelines and Limitations

The Cisco LoRaWAN pluggable modules have the following guidelines and limitations:

- Support is available with IOS-XE release 17.10.1 and later
- Physical OIR is not supported
- GPS Coordinates locking is mandatory for the latest Common Packet Forwarder (CPF) application to work on the PIM module

The following guidelines and limitations apply to the IR1101:

- The Cisco LoRaWAN module can be installed in the Base module or Expansion module
- The Cisco LoRaWAN module is supported in both the IRM-1100-SP and IRM-1100-SPMI expansion modules
- Only one Cisco LoRaWAN module is supported. Any combination of two or more Cisco LoRaWAN modules is not supported

Important The Cisco LoRaWAN module can not be used on the IR1101 when running on the npe IOS XE software image.

GPS Channel Plans

GPS check for verification of channel plans is included.

Note This table is derived from the LoRaWAN Regional Parameters document, version RP2-1.0.2.

Note The CPF feature is intended to operate only when a GPS fix is actively available or has been stored from an earlier fix. The location derived from the GPS fix must be in one of the countries listed in the table below. If not, the radio will not turn on. This does not apply to Actility LRR since the channel plan is configured on the network server.

Countries supported by GPS check include:

Code	Name	Channel plan
AL	Albania	EU868
AD	Andorra	EU868
AM	Armenia	EU868
AR	Argentina	AU915-928
AT	Austria	EU868
AU	Australia	AU915 (default) AS923
AZ	Azerbaijan	EU868
BY	Belarus	EU868
BE	Belgium	EU868
BA	Bosnia	EU868
BN	Brunei	EU868
BG	Bulgaria	EU868
KH	Cambodia	EU868
CA	Canada	US915 (default) AU915
CN	China	AS923
HR	Croatia	EU868
CY	Cyprus	EU868
CZ	Czech Republic	EU868
DK	Denmark	EU868
EE	Estonia	EU868

Code	Name	Channel plan
FI	Finland	EU868
FR	France	EU868
DE	Germany	EU868
GR	Greece	EU868
HK	Hongkong	EU868
HU	Hungary	EU868
IS	Iceland	EU868
IE	Ireland	EU868
IN	India	IN865
IT	Italy	EU868
JP	Japan	AS923
LA	Laos	EU868
LV	Latvia	EU868
LI	Liechtenstein	EU868
LT	Lithuania	EU868
LU	Luxembourg	EU868
MK	Macedonia	EU868
MY	Malaysia	EU868
MX	Mexico	US915
MD	Moldova	EU868
ME	Montenegro	EU868
NL	Netherlands	EU868
NZ	New Zealand	AS923 AU915
NO	Norway	EU868
PL	Poland	EU868
PT	Portugal	EU868
PR	Puerto Rico	US915
RO	Romania	EU868

Code	Name	Channel plan
RS	Serbia	EU868
SG	Singapore	EU868
SK	Slovakia	EU868
SI	Slovenia	EU868
ZA	South Africa	EU868
ES	Spain	EU868
SE	Sweden	EU868
CH	Switzerland	EU868
TH	Thailand	EU868
TR	Turkey	EU868
GB	United Kingdom	EU868
UA	Ukraine	EU868
US	United States	US915 (default) AU915
VA	Vatican City	EU868
VN	Vietnam	EU868

Note Refer to the LoRa Alliance Technical Specifications for more information.

Installing the P-LPWA-XXX Pluggable Module

The router may have a blank plate covering the Pluggable Module slot. This will need to be removed prior to installing the P-LPWA-XXX module.

Procedure

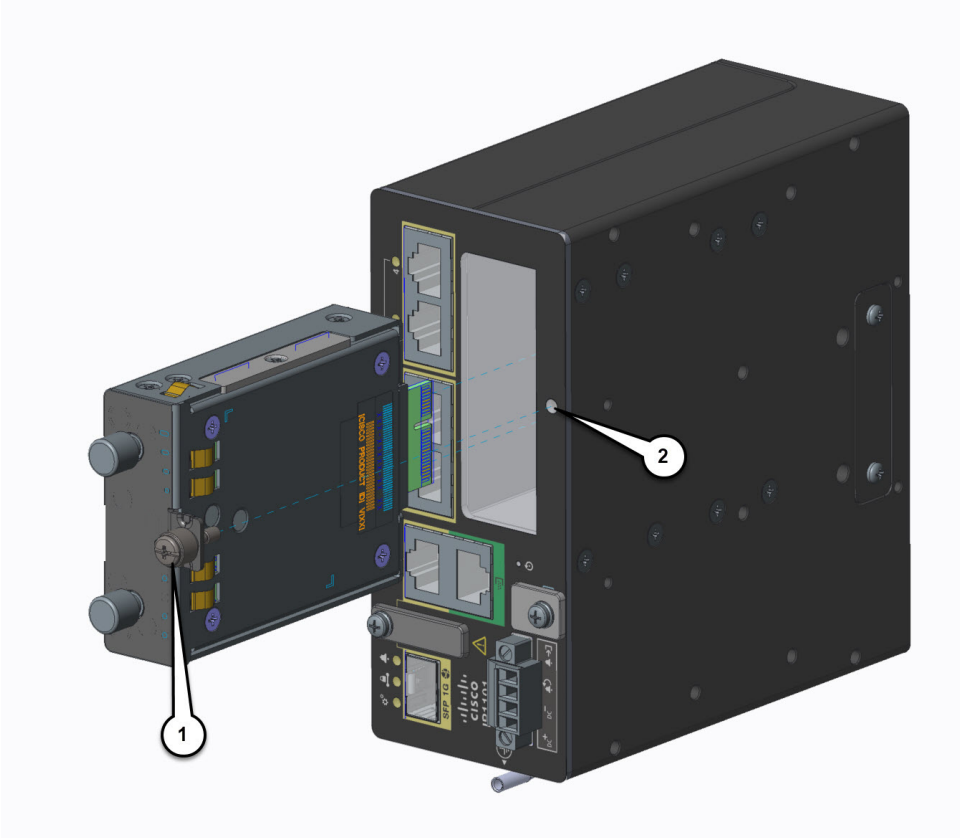
Step 1 Remove the blank plate by unscrewing the latch lock screw (**1**) that holds the plate secure. Refer to the following figure.

Figure 3: Latch Lock Screw

Step 2 Slide the blank plate out of the device.

Step 3 Slide the Pluggable Module into the device as shown in the following figure. The latch lock screw (**1**) aligns with the screw hole (**2**) on the front of the device. Push the Pluggable Module all the way into the device until you feel it seat, and then torque the latch lock screw 8-10 inch-pound (0.9 to 1.1 newton meter).

Figure 4: Pluggable Module Insert



Step 4 Attach your antennas to the ports on the pluggable module. There are different instructions for each antenna type, be sure to consult the Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide.

Step 5 If no antennas are being installed on a port, make sure the antenna caps are installed on the connector.

Deployment Scenarios on the IR1101

The IR1101 has two sides that an expansion module can mount to. The top is called the Expansion side, and the bottom is called the Compute side. If the expansion module is connected to the top, then it is referred to as the EM side. If the expansion module is connected on the bottom, then it is referred to as the CM side.

Note The CM side support will be added in a future release.

Functionality differs depending on which side the expansion module is attached to, how many, and types of expansion modules are in use.

Additional information can be found in the Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide.

Scenario One

In this scenario, the Cisco LoRaWAN module is installed in the IR1101 Base unit. See the following figure:

In this configuration the Cisco LoRaWAN module has full functionality. The interface numbering in this scenario is LORAWAN 0/1/0.

Scenario Two

In this scenario, the Cisco LoRaWAN module is mounted on the Expansion side, or the top. See the following figure:

In this configuration the LoRaWAN module has full functionality. The interface numbering in this scenario is LORAWAN 0/3/0.

Inventory Details Based on Deployment

The output of the different **show** commands will show different details based upon which side of the IR1101 base unit it is attached to.

```
Router# show inventory

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9          , VID: V03  , SN: FCW2424P05J

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9          , VID: V03  , SN: FOC24233KEB

NAME: "module subslot 0/0", DESCR: "IR1101-ES-6S"
PID: IR1101-ES-6S       , VID: V01  , SN:

NAME: "module subslot 0/1", DESCR: "P-LTEA-EA Module"
PID: P-LTEA-EA          , VID: V02  , SN: FOC23044M0J

NAME: "Modem on Cellular0/1/0", DESCR: "Sierra Wireless EM7455"
PID: EM7455             , VID: 1.0  , SN: 356129070601460

NAME: "module subslot 0/3", DESCR: "P-LPWA-900 Module"
```

```
PID: P-LPWA-900         , VID: V00  , SN: FOC25520G96

NAME: "Module 4 - Expansion Module", DESCR: "IR1100 expansion module with Pluggable slot
and SFP"
PID: IRM-1100-SP        , VID: V02  , SN: FCW2544Z0M3
Router#
```

```
Router#show platform
Chassis type: IR1101-K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         IR1101-K9           ok                    21:18:40
 0/0      IR1101-ES-6S        ok                    21:17:20
 0/1      P-LTEA-EA           ok                    21:17:20
 0/3      P-LPWA-900          ok                    21:17:20
R0        IR1101-K9           ok, active            21:18:40
F0        IR1101-K9           ok, active            21:18:40
P0        PWR-12V             ok                    21:18:05
Router#
```

```
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   172.27.127.211  YES NVRAM  up                    up
FastEthernet0/0/1      unassigned      YES unset  down                  down
FastEthernet0/0/2      unassigned      YES unset  down                  down
FastEthernet0/0/3      unassigned      YES unset  down                  down
FastEthernet0/0/4      unassigned      YES unset  down                  down
GigabitEthernet0/0/5   unassigned      YES unset  down                  down
Cellular0/1/0          unassigned      YES NVRAM  up                    up
Cellular0/1/1          unassigned      YES NVRAM  down                  down
LORAWAN0/3/0           unassigned      YES NVRAM  up                    up
Async0/2/0             unassigned      YES unset  up                    down
Tunnel1                unassigned      YES unset  up                    down
Tunnel11               31.31.31.1      YES NVRAM  up                    up
Tunnel12               30.30.30.1      YES NVRAM  up                    up
VirtualPortGroup0      192.168.2.1     YES NVRAM  up                    up
Vlan1                  unassigned      YES unset  up                    down
Router#
```

Cisco LoRaWAN Pluggable Interface Module LEDs

There are two LEDs on the front the PIM module. The LED on the left is the Power LED, and the LED on the right is the Status LED.

Figure 5: P-LPWA-xxx LEDs

The following tables describe the LEDs:

LoRa Power LED	Description
Green	Operational with the radio on.
Amber	Module is powering up.
Off	No power.

LoRa Status LED	Description
Green	PIM fully configured. LoRa Interface Operational.
Red	PIM interface error encountered, or a problem occured during configuration.
Off	PIM not fully configured.

The LED status is also available through the CLI.

```
Router#show led
YSTEM LED : Green

Custom LED : Off

VPN LED : Off

ALARM LED : Off

GigabitEthernet0/0/0 LED : On
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off

LORAWAN0/1/0
Lorawan Module Power LED : GREEN
Lorawan Module Status LED : GREEN
Router#
```

Supported Antenna and RF Accessories

This section shows details for the supported antennas, cables, and lightning arrestors used in a deployment with the P-LPWA-XXX Pluggable Module.

Table 2: LoRaWAN Antennas

Cisco PID	Connector	Frequency	Peak Gain	Polarization	Radiation Pattern
ANT-LPWA-SMA-D	SMA(m)	863 – 928 MHz	1.0 dBi	Linear, Vertical	Omnidirectional
ANT-LPWA-DB-O-N-5	N(f)	863 – 928 MHz	5.6 dBi	Linear, Vertical	Omnidirectional
ANT-WPAN-OD-OUT-N	N(m)	863 – 928 MHz	1.5 dBi	Linear, Vertical	Omnidirectional

Table 3: GNSS Antennas

Cisco PID	Connector	Frequency	Peak Gain	Polarization	Radiation Pattern
GPS-ACT-ANTM-SMA	SMA(m) with 17 ft. integrated cable.	1575.42 ± 1 MHz	4 dBic	RHCP	Hemispheric

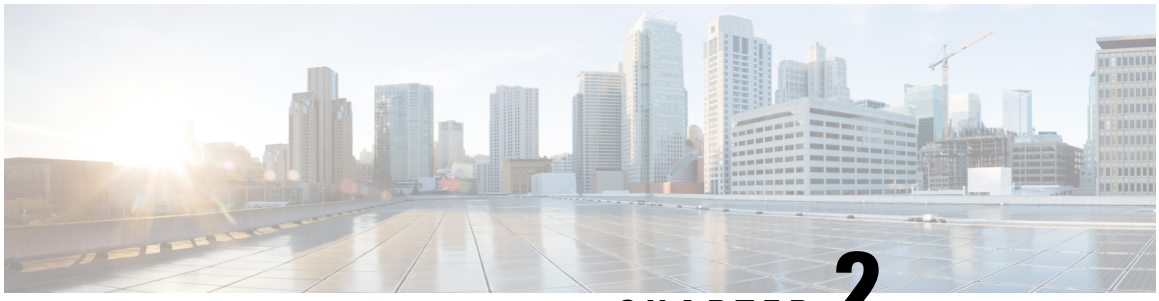
Table 4: Coaxial Cables

Cisco PID	Description
CAB-L240-10-SM-NM	10 ft. LMR-240-DB/FR/CMR, SMA(m)-STR to N(m)-STR
CAB-L400-5-N-N	5 ft. LMR-400-DB, N(m)-STR to N(m)-R/A
CAB-L400-5-N-NS	5 ft. LMR-400-DB, N(m)-STR to N(m)-STR
AIR-CAB010LL-N	10 ft. LMR-400-DB, N(m)-STR to N(m)-STR
CAB-L400-20-N-N	20 ft. LMR-400-DB, N(m)-STR to N(m)-RA
AIR-CAB025HZ-N	25 ft. LMR-400-DB/FR/CMR, N(m)-STR to N(m)-RA
CAB-L600-30-N-N	30 ft. LMR-600-DB, N(m)-STR to N(m)-RA

Table 5: Lightning Arrestors

Cisco PID	Connectors	Description
CGR-LA-NM-NF	N(m)-STR to N(f)-STR	DC to 7 GHz, GDT type, bidirectional
CGR-LA-NF-NF	N(f)-STR to N(f)-STR	DC to 7 GHz, GDT type, bidirectional

For installation instructions and detailed information on any of these antennas, refer to the antenna data sheet on Cisco.com, or see the Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide.



CHAPTER 2

Configuring the Pluggable Module

This chapter contains the following sections:

LPWA Interface Configuration

The P-LPWA-800 and P-LPWA-900 modules can be managed by command line interface (CLI), or the Cisco IOS XE Web User Interface (WebUI).

Note GPS is mandatory for the Common Packet Forwarder (CPF) application to work. Please connect the Lora module GPS antenna, and check the GPS status using the below command before installing the CPF application.

```
Router#show lorawan 0/1/0 gps
Recorded GNSS Info at 2022-09-13 19:20:50 UTC

GNSS Location:
Latitude: 37 Deg 25 Min 5.937 Sec North (37.418316)
Longitude: 121 Deg 55 Min 9.714 Sec West (-121.919365)
Height: 37.0m

Router#
```

The following is an example of GPS Configuration:

```
interface LORAWAN0/1/0
no ip address
common-packet-forwarder profile
country UNITEDSTATES
region-channel-plan US915
gateway-id 69
lns-ip 172.27.127.209
lns-port 6080
log-level xdebug lines 240
gps enable
cpf enable
arp timeout 0
no mop enabled
```

```
no mop sysid
end
```

To clear the GPS information use the following command:

```
Router#clear lorawan 0/1/0 cpf location-info
Router#
```

Common Packet Forwarder Configuration Steps

Additional information can be found at Managing Packet Forwarder.

Follow these steps to configure the interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**int loraWAN** *interface* **Example:** `Router(config)# int loraWAN 0/1/0`	Enters LoraWan interface config mode.
Step 3	**common-packet-forwarder profile** **Example:** `Router(config-if)# common-packet-forwarder profile`	Configures parameters for the CPF.
Step 4	**region-channel-plan** <*number*> **Example:** `Router(config-if-lorawan-cpf)#region-channel-plan US915`	Configures the regional channel plan code.
Step 5	**gateway-id** <*number*> **Example:** `Router(config-if-lorawan-cpf)# gateway-id 69`	Configures gateway id used for CPF.
Step 6	**lns-ip** <*ip-address*> **Example:** `Router(config-if-lorawan-cpf)#lns-ip 172.27.127.209`	Configures Lora network server IP address.
Step 7	**lns-port** <*port-number*> **Example:** `Router(config-if-lorawan-cpf)# lns-port 6080`	Configures Lora network server port number.
Step 8	**cpf enable**	Starts the CPF.

	Command or Action	Purpose
	Example: `Router(config-if-lorawan-cpf)# cpf enable`	**Note** This configuration will ONLY take effect after exiting from current sub-mode.
Step 9	**exit** **Example:** `Router(config-if-lorawan-cpf)# exit`	Exits the CPF profile block and updates the configuration.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits from interface config mode.
Step 11	**exit** **Example:** `Router# exit`	Exits from config mode.

Default Configuration

The following is an example of a default configuration for the lorawan interface.

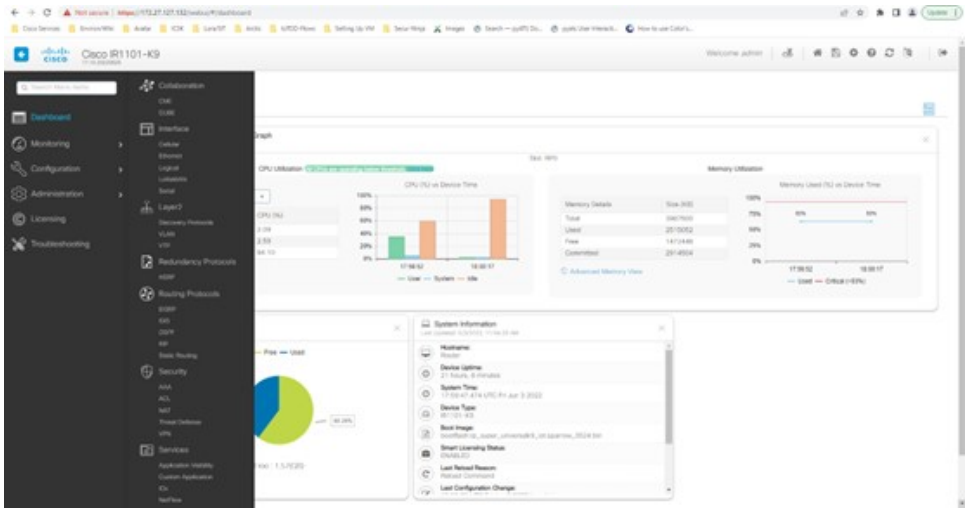
```
Router#sh run int lorawan 0/3/0
Building configuration...

Current configuration : 192 bytes
!
interface LORAWAN0/3/0
 no ip address
 common-packet-forwarder profile
  gateway-id 69
  lns-ip 172.27.127.209
  lns-port 6080
  cpf enable
 arp timeout 0
 no mop enabled
 no mop sysid
end
Router#
```

Configuring the Interface using the WebUI

Use the following steps to configure the Cisco lorawan interface through the WebUI.

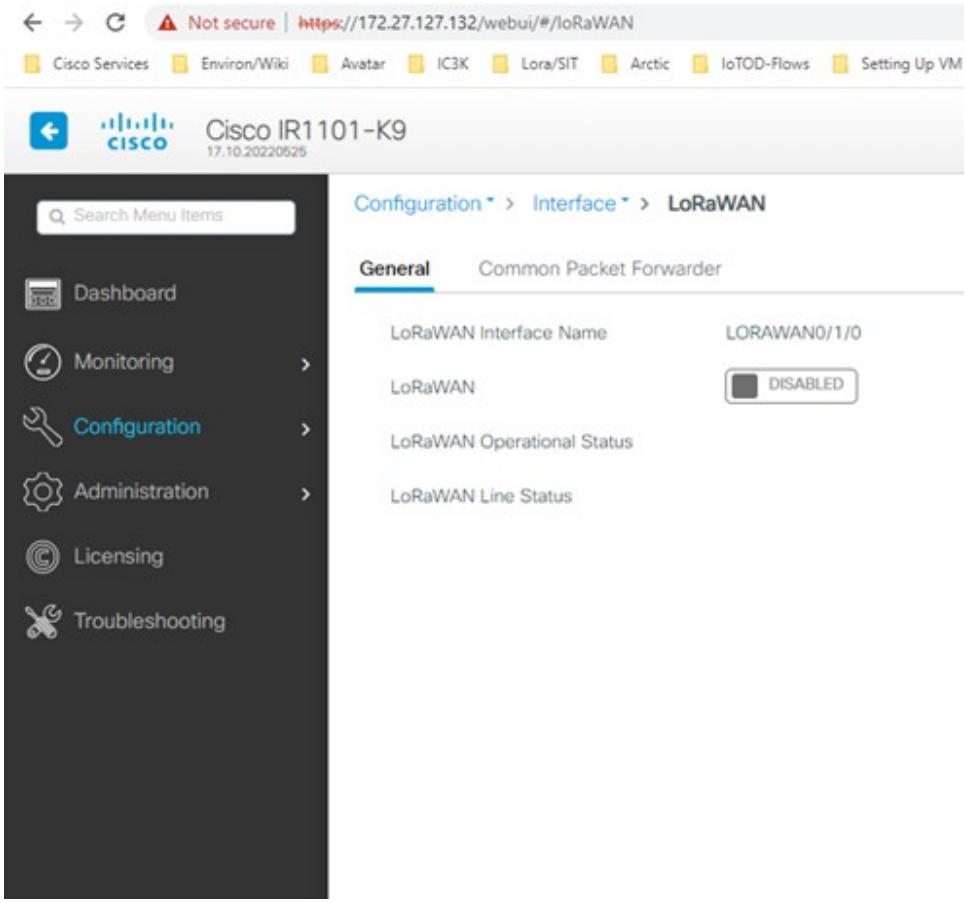
Procedure

Step 1 After launching the WebUI, navigate to **Configuration > LoRaWAN**.

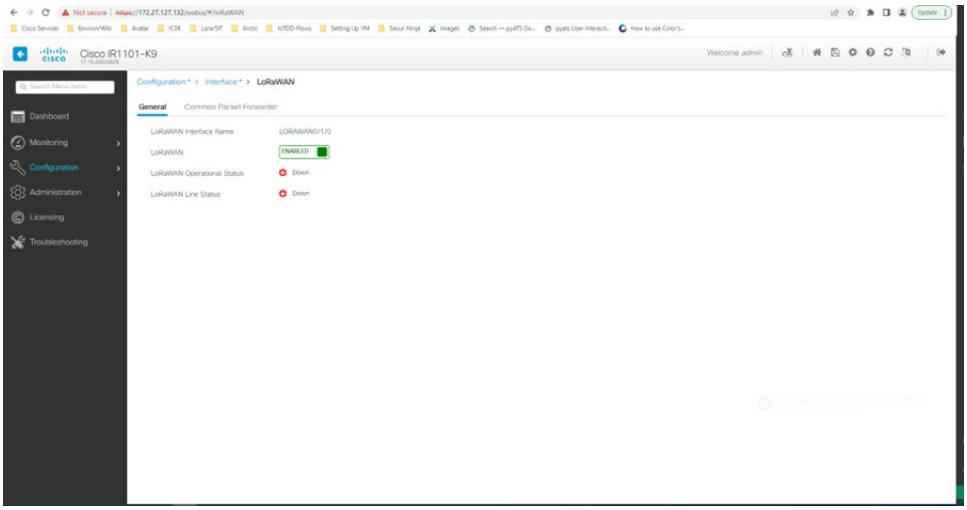


For details about using the WebUI, see Web User Interface (WebUI) in the IR1101 Software Configuration Guide.

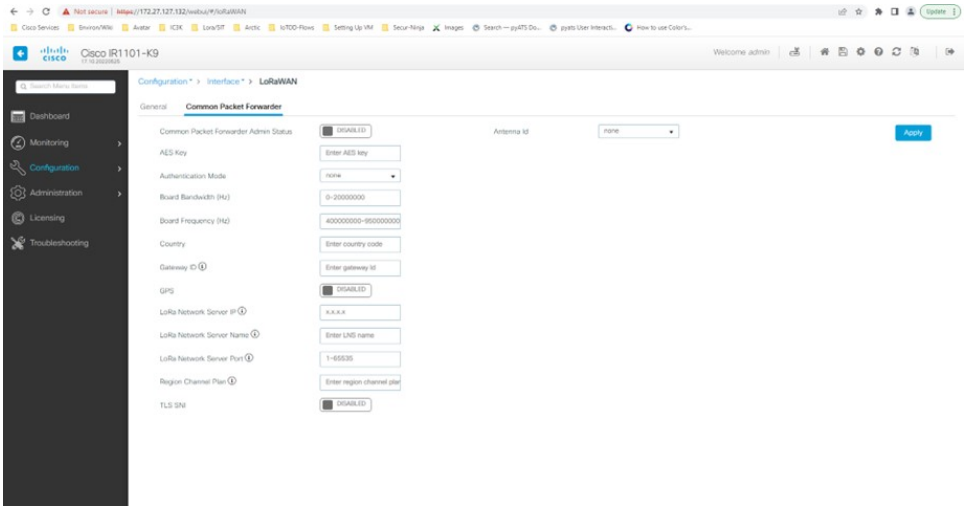
Step 2 Double click on the **LoRaWAN** interface.



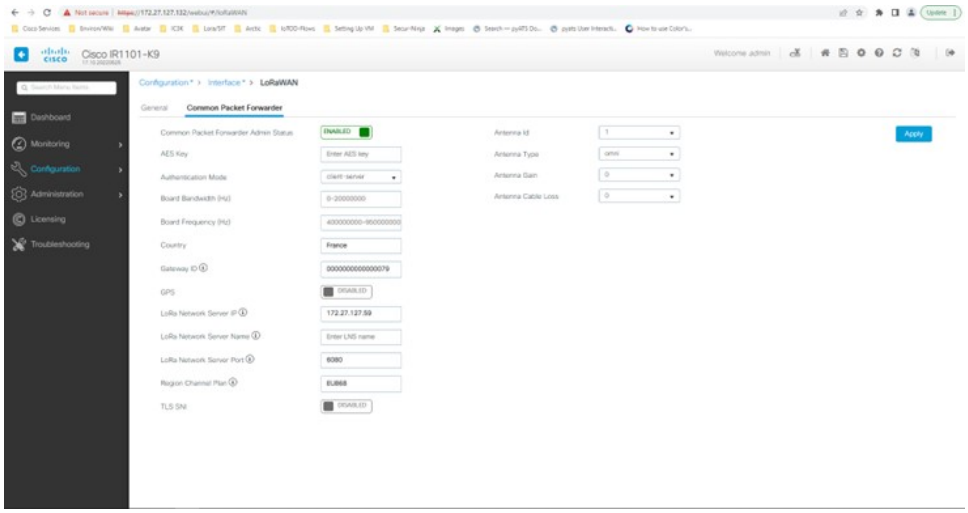
Step 3 Enable the Cisco lorawan interface.



Step 4 Click on the **Common Packet Forwarder** tab to add the CPF configuration.



Step 5 Add the CPF configuration and set the Common Packet Forwarder Admin Status to ENABLED.



What to do next

For the Application deployment process using the Local Manager, please refer to Cisco IOx Local Manager Workflows.

Common Packet Forwarder Application Hosting for LoRa Technology

To configure application hosting, enable IOx and configure a VirtualPortGroup to a Layer 3 data port. These steps are described in the following sections.

Enable IOx

Perform the following steps to enable access to Cisco IOx Local Manager. IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enable privileged EXEC mode
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**iox** **Example:** `Router(config)#iox`	Enable Cisco IOx
Step 4	**ip http server** **Example:** `Router(config)#ip http server`	Enable the HTTP server on your IPv4 or IPv6 system.
Step 5	**ip http secure-server** **Example:** `Router(config)#ip http secure-server`	Enable a secure HTTP (HTTPS) server.
Step 6	**username** *name* **privilege** *level* **password** {0 | 7 | *user-password* } *encrypted-password* **Example:** `Router(config)#username cisco privilege 15 password 0 cisco`	Establish a username-based authentication system and privilege level. The username privilege level must be configured as 15.
Step 7	**end** **Example:** `Router(config-if)#end`	Exit the interface configuration mode and return to the privileged EXEC mode.

Configure a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. A VirtualPortGroup interface is a virtual interface that connects the application hosting network to the IOS routing domain. VirutalPortGroups and Layer 3 data ports must be on different subnets.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip routing** **Example:** `Router(config)#ip routing`	Enable IP routing. The ip routing command must be enabled to allow external routing on Layer 3 data ports.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Router(config)#interface gigabitethernet 0/0/0`	Configure an interface and enter interface configuration mode.
Step 5	**no switchport** **Example:** `Router(config-if)#no switchport`	Place the interface in Layer 3 mode and make it operate more like a router interface than a switch port.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config)#ip address 10.1.1.1 255.255.255.0`	Configure an IP address for the interface.
Step 7	**exit** **Example:** `Router(config-if)#exit`	Exit interface configuration mode and return to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)#interface virtualportgroup 0`	Configure an interface and enter interface configuration mode.
Step 9	**ip address** *ip-address mask* **Example:** `Router(config-if)#ip address 192.168.0.1 255.255.255.0`	Configure an IP address for the interface.
Step 10	**end** **Example:** `Router(config-if)#end`	Exit interface configuration mode and return to global configuration mode.

Configure Application Networking

Application vNIC interface is the standard Ethernet interface inside the container that connects to the platform data plane for the application to send and receive packets.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.
Step 3	**app-hosting appid** *app1* **Example:** `Router(config)#app-hosting appid app1`	Configure the application and enter the application configuration mode.
Step 4	**app-vnic** *options* **Example:** `Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0`	Configure the application interface and the gateway of the application.
Step 5	**guest-ipaddress** *ip-address mask* **Example:** `Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.2 netmask 255.255.255.0`	Configure the application Ethernet interface IP address.
Step 6	**app-default-gateway** *options* **Example:** `Router(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0`	Configure the default gateway for the application.
Step 7	**end** **Example:** `Router#end`	Exit the global configuration mode and return to the privileged EXEC mode.

Application Lifecycle Management

This section describes the process of installing and uninstalling apps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.

	Command or Action	Purpose
Step 3	**app-hosting install appid** *application-name* **package** *package-path* **Example:** `Router(config)#app-hosting install appid CPFAPP package flash:cpfv5.tar`	Installs an app from the specified location. The app can be installed from any local storage location such as flash, bootflash, and usbflash0.
Step 4	**app-hosting activate appid** *application-name* **Example:** `Router#app-hosting activate appid CPFAPP`	Activate the application. This command validates all application resource requests, and if all resources are available, activates the application. If all resources are not available, the activation fails.
Step 5	**app-hosting start appid** *application-name* **Example:** `Router#app-hosting start appid CPFAPP`	Start the application. This command activates the application start-up scripts.
Step 6	**app-hosting stop appid** *application-name* **Example:** `Router#app-hosting stop appid CPFAPP`	Stop the application.
Step 7	**app-hosting deactivate appid** *application-name* **Example:** `Router#app-hosting deactivate appid CPFAPP`	Deactivates all resources that are allocated for the application.
Step 8	**app-hosting uninstall appid** *application-name* **Example:** `Router(config)#app-hosting uninstall appid CPFAPP`	Uninstalls all packaging and images that are stored and removes all changes and updates to the application.

Verifying the Application Hosting Configuration

This section shows commands to verify the application hosting configuration.

Display the status of all IOx services

```
Router#show iox-service

IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

Router#
```

Display detailed information about the application

```
Router#show app-hosting detail
pp id                          : cp
Owner                          : iox
State                          : RUNNING

Application
  Type                         : docker
  Name                         : cpf
  Version                      : vl
  Description                  : buildkit.dockerfile.vO
  Author                       :
  Path                         : bootflash:cpfv5.tar
  URL Path                     :
  Multicast                    : yes
 Activated profile name        :custom

Resource reservation
  Memory                       :128 MB
  Disk                         :10 MB
  CPU                          :400 units
  CPU-percent                  :35 %
  VCPU                         :1

Platform resource profiles
  Profile Name          CPU(unit)  Memory(MB)  Disk(MB)
  ----------------------------------------------------------------

Attached devices
  Type            Name                Alias
  ---------------------------------------
  serial/shell     iox_console_shell   serial0
  serial/aux       iox_console_aux     serial1
  serial/syslog    iox_syslog          serial2
  serial/trace     iox_trace           serial3

Network interfaces
-----------------------------------------------
eth0:
  MAC address               : 52:54:dd:f2:f4:87
  IPv4 address              : 192.168.0.9
  IPv6 address              ::
  Network name              : VPGO


Docker
------
Run-time information
  Command                   :
  Entry-point               : /station/cpf
  Run options in use        : --device /dev/lorawan_ttyl:/dev/ttyACMO -v
/bootflash/lorawan_0:/cpf/
  Package run options       :

Application health information
  Status                    : 0
  Last probe error          :
  Last probe output         :
```

Display the list of applications and their statuses

```
Router#show app-hosting list
App id State
------------------------------------------
CPFAPP RUNNING
```

Use the Console command to connect to the application

Press **Ctrl+C** three times to disconnect from the console.

```
Router# app-hosting app-hosting connect appid CPFAPP console
Connected to appliance. Exit using ^c^c^c
root@ir510-lxc:~#
root@ir510-lxc:~#
root@ir510-lxc:~#
root@ir510-lxc:~#
root@ir510-lxc:~#
root@ir510-lxc:~# IR11014006#
```

Actility Packet Forwarder Application Hosting for LoRa Technology

The following are prerequisites for configuring application hosting. There is a new process for ssh key sharing between the container and host.

Perform the following on the host:

Add a username and password.

```
config terminal
username actility privilege 15 password 0 Actility_Password
exit
```

Run the docker container with the following options:

- device /dev/ttyACM0:/dev/ttyACM0
- env HOST_IP_ADDR=192.168.42.11
- env HOST_USER=actility
- env HOST_SETUP_PASSWORD=actilityPassword

In the docker container options above, note the default ip address, username, and password. Change these to match your configuration.

Note After the first installation you do not have a password for the actility user (username actility privilege 15). If you want to reinstall ThingPark Long Range Relay (LRR) software, you will have to set **username actility privilege 15 password 0** *actilityPassword* again.

To configure application hosting, enable IOx and configure a VirtualPortGroup to a Layer 3 data port. These steps are described in the following sections.

Enable IOx

Perform the following steps to enable access to Cisco IOx Local Manager. IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>enable`	Enable privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters global configuration mode.
Step 3	**iox** **Example:** `Router(config)#iox`	Enable Cisco IOx.
Step 4	**ip http server** **Example:** `Router(config)#ip http server`	Enable the HTTP server on your IPv4 or IPv6 system.
Step 5	**ip http secure-server** **Example:** `Router(config)#ip http secure-server`	Enable a secure HTTP (HTTPS) server.
Step 6	**username** *name* **privilege** *level* **password** {0 | 7 | *user-password* } *encrypted-password* **Example:** `Router(config)#username cisco privilege 15 password 0 cisco`	Establish a username-based authentication system and privilege level. The username privilege level must be configured as 15.
Step 7	**end** **Example:** `Router(config-if)#end`	Exit the interface configuration mode and return to the privileged EXEC mode.

Configure a VirtualPortGroup to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more VirtualPortGroups or containers. A VirtualPortGroup interface is a virtual interface that connects the application hosting network to the IOS routing domain. VirutalPortGroups and Layer 3 data ports must be on different subnets.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip routing** **Example:** `Router(config)#ip routing`	Enable IP routing. The ip routing command must be enabled to allow external routing on Layer 3 data ports.
Step 4	**interface** *type number* **Example:** `Router(config)#interface gigabitethernet 0/0/0`	Configure an interface and enter interface configuration mode.
Step 5	**no switchport** **Example:** `Router(config-if)#no switchport`	Place the interface in Layer 3 mode and make it operate more like a router interface than a switch port.
Step 6	**ip address dhcp** **Example:** `Router(config)#ip address dhcp`	Configure an IP address for the interface.
Step 7	**exit** **Example:** `Router(config-if)#exit`	Exit interface configuration mode and return to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)#interface virtualportgroup 0`	Configure an interface and enter interface configuration mode.
Step 9	**ip address** *ip-address mask* **Example:** `Router(config-if)#ip address 192.168.2.1 255.255.255.0`	Exit interface configuration mode and return to global configuration mode.
Step 10	**end** **Example:** `Router(config-if)#end`	Exit interface configuration mode and return to global configuration mode.

Configure Application Networking

Application vNIC interface is the standard Ethernet interface inside the container that connects to the platform data plane for the application to send and receive packets.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router#configure terminal`	Enters global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.
Step 3	**app-hosting appid** *app1* **Example:** `Router(config)#app-hosting appid app1`	Configure the application and enter the application configuration mode.
Step 4	**app-vnic** *options* **Example:** `Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0`	Configure the application interface and the gateway of the application.
Step 5	**guest-ipaddress** *ip-address mask* **Example:** `Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.9 netmask 255.255.255.0`	Configure the application Ethernet interface IP address.
Step 6	**app-default-gateway** *options* **Example:** `Router(config-app-hosting-gateway0)#app-default-gateway 192.168.2.1 guest-interface 0`	Configure the default gateway for the application.
Step 7	**end** **Example:** `Router#end`	Exit the global configuration mode and return to the privileged EXEC mode.

Application Lifecycle Management

This section describes the process of installing and uninstalling apps.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enable privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode, and then enter configuration commands, one per line. Press CTRL-Z when you are finished entering configuration commands.
Step 3	**app-hosting install appid** *application-name* **package** *package-path* **Example:** `Router(config)#app-hosting install appid APFAPP package flash:actility_tar_gz.tar`	Installs the app from the specified location. The app can be installed from any local storage location such as flash, bootflash, and usbflash0.
Step 4	**app-hosting activate appid** *application-name* **Example:** `Router#app-hosting activate appid APFAPP`	Activate the application. This command validates all application resource requests, and if all resources are available, activates the application. If all resources are not available, the activation fails.
Step 5	**app-hosting start appid** *application-name* **Example:** `Router#app-hosting start appid APFAPP`	Start the application. This command activates the application start-up scripts.
Step 6	**app-hosting stop appid** *application-name* **Example:** `Router#app-hosting stop appid APFAPP`	Stop the application.
Step 7	**app-hosting deactivate appid** *application-name* **Example:** `Router#app-hosting deactivate appid APFAPP`	Deactivates all resources that are allocated for the application.
Step 8	**app-hosting uninstall appid** *application-name* **Example:** `Router(config)#app-hosting uninstall appid APFAPP`	Uninstalls all packaging and images that are stored and removes all changes and updates to the application.

Verifying the Application Hosting Configuration

This section shows commands to verify the application hosting configuration.

Display the status of all IOx services

```
Router#show iox-service
```

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

Router#
```

Display detailed information about the application

```
Router#show app-hosting detail
 App id                 : APFC1
Owner                   : iox
State                   : RUNNING
Application
  Type                  : docker
  Name                  : base-rootfs-runtime-actility
  Version               : latest
  Description           : Actility LRR
  Author                : Actility
  Path                  : bootflash:actility_lrr_76.tar.gz
  URL Path              :
  Multicast             : yes
Activated profile name  : custom

Resource reservation
  Memory                : 64 MB
  Disk                  : 2 MB
  CPU                   : 50 units
  CPU-percent           : 5 %
  VCPU                  : 1

Platform resource profiles
  Profile Name                  CPU(unit)  Memory(MB)  Disk(MB)
  ----------------------------------------------------------------

Attached devices
  Type              Name               Alias
  ---------------------------------------------
  serial/shell     iox_console_shell   serial0
  serial/aux       iox_console_aux     serial1
  serial/syslog    iox_syslog          serial2
  serial/trace     iox_trace           serial3

Network interfaces
   ---------------------------------------
eth0:
   MAC address          : 52:54:dd:16:24:0a
   IPv4 address         : 192.168.2.9
   IPv6 address         : ::
   Network name         : VPG0


Docker
------
Run-time information
  Command               :
  Entry-point           :  /etc/init.d/lrr_iox_top start
  Run options in use    : --device /dev/ttyACM0:/dev/ttyACM0 --env HOST_IP_ADDR=192.168.2.1
 --env HOST_USER=actility --env HOST_SETUP_PASSWORD=actilityPassword
  Package run options   :
```

```
Application health information
  Status               : 0
  Last probe error     :
  Last probe output    :

Router#
```

Display the list of applications and their statuses

```
Router#show app-hosting list
App id State
------------------------------------------
APFAPP RUNNING
```

Use the following command to connect to the application

Press **Ctrl+C** three times to disconnect the console.

```
Router# app-hosting app-hosting connect appid APFAPP session
/home/actility/var/log/lrr

/var/volatile/log/_LRRLOG # pwd
/home/actility/var/log/lrr

/var/volatile/log/_LRRLOG # ls -lrt
-rw-r--r--    1 root     root            19 Jul  7 0646 SHELL.log
-rw-r--r--    1 root     support         53 Jul  7 0647 suplog.log
-rw-r--r--    1 root     support         99 Jul  7 0648 pkiconfig.txt
-rw-r--r--    1 root     root           430 Jul  7 0720 lrr_startup_service.log
-rw-r--r--    2 root     root          1620 Jul  7 0721 gwmgr_04.log
-rw-r--r--    2 root     root          1620 Jul  7 0721 gwmgr.log
-rw-r--r--    1 root     root          1657 Jul  7 0721 radioparams.txt
-rw-r--r--    1 root     root          2227 Jul  7 0721 logicchan.txt
-rw-r--r--    1 root     root          1118 Jul  7 1721 stat.html
-rw-r--r--    2 root     root         50515 Jul  7 1721 TRACE_04.log
-rw-r--r--    2 root     root         50515 Jul  7 1721 TRACE.log
-rw-r--r--    1 root     root            64 Jul  7 1723 lrcstatuslink.txt
/var/volatile/log/_LRRLOG #
```

Show app hosting in the running configuration

```
Router#show running-config | sec app-hosting
 action 2 cli command "app-hosting stop appid APFC1"
 action 4 cli command "app-hosting start appid APFC1"
app-hosting appid APFC1
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.2.9 netmask 255.255.255.0
 app-default-gateway 192.168.2.1 guest-interface 0
 app-resource docker
  run-opts 1 "--device /dev/ttyACM0:/dev/ttyACM0"
  run-opts 2 "--env HOST_IP_ADDR=192.168.2.1"
  run-opts 3 "--env HOST_USER=actility"
  run-opts 4 "--env HOST_SETUP_PASSWORD=actilityPassword"
Router#
```

Sample Running Configuration

The following example if from an IR1101.

```
Router#show running-config brief
Building configuration...

Current configuration  7651 bytes
!
! Last configuration change at 072004 UTC Thu Jul 7 2022 by actility
! NVRAM config last updated at 065725 UTC Thu Jul 7 2022 by actility
!
version 17.9
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform hardware throughput level 250M
platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot system flashir1101-universalk9.S2C.SSA.bin
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
aaa session-id common
!
!
login block-for 60 attempts 3 within 30
login delay 3
login on-success log
ipv6 unicast-routing
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint TP-self-signed-1150468717
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1150468717
 revocation-check none
 rsakeypair TP-self-signed-1150468717
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint ActilityTP-slrc
 enrollment terminal
 revocation-check none
!
crypto pki trustpoint ActilityTP
 enrollment pkcs12
 revocation-check crl
 rsakeypair ActilityTP
```

```
!
crypto pki trustpoint ActilityTP-rrr1
 revocation-check crl
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 subject-name co slrc1_prod-us_actility-tpe-ope
!
crypto pki certificate map FlexVPN_Cert_Map 2
 subject-name co slrc2_prod-us_actility-tpe-ope
!
crypto pki certificate chain TP-self-signed-1150468717
 certificate self-signed 01
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
crypto pki certificate chain ActilityTP-slrc
 certificate ca 61A845069BBFF60B
crypto pki certificate chain ActilityTP
 certificate 06BF5FDCF5EBD17C
 certificate ca 3A96CABF858AAD9A
crypto pki certificate chain ActilityTP-rrr1
 certificate ca 00F35AC229699BABA8
!
!
no license feature hseck9
license udi pid IR1101-K9 sn FCW24160HQ7
license boot level network-advantage
memory free low-watermark processor 45069
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
username admin privilege 15 password 0 cisco
username iox privilege 15 password 0 iox
username dockeruser
username actility privilege 15
!
redundancy
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint ActilityTP sign
 pki trustpoint ActilityTP-rrr1 verify
 pki trustpoint ActilityTP-slrc verify
 dpd 30 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 dpd 30 3 periodic
crypto ikev2 fragmentation mtu 1260
!
controller Cellular 0/3/0
!
!
vlan internal allocation policy ascending
!
!
```

```
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
interface Tunnel201
 ip address negotiated
 ip nat outside
 ipv6 enable
 tunnel source GigabitEthernet0/0/0
 tunnel mode ipsec dual-overlay
 tunnel destination 52.200.161.236
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface Tunnel202
 ip address negotiated
 ip nat outside
 ipv6 enable
 tunnel source GigabitEthernet0/0/0
 tunnel mode ipsec dual-overlay
 tunnel destination 54.226.90.83
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup0
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip dhcp client client-id ascii cisco-ac4a.67f9.ae00-Gi0/0/0
 ip address dhcp
 ip nat outside
 ipv6 dhcp client request vendor
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface GigabitEthernet0/0/5
!
interface Cellular0/3/0
 description backup_WAN
 ip address negotiated
 ip nat outside
 ip tcp adjust-mss 1460
 load-interval 30
 shutdown
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 enable
```

```
 pulse-time 1
!
interface Cellular0/3/1
 no ip address
!
interface Vlan1
 no ip address
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
interface LORAWAN0/1/0
 no ip address
 shutdown
 arp timeout 0
 no mop enabled
 no mop sysid
!
iox
ip forward-protocol nd
ip tcp selective-ack
ip tcp mss 1460
ip tcp window-size 131072
ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip tftp source-interface GigabitEthernet0/0/0
ip nat inside source list Tunnel201 interface Tunnel201 overload
ip nat inside source list Tunnel202 interface Tunnel202 overload
ip nat inside source list internetacces_Fromdocker interface GigabitEthernet0/0/0 overload
ip nat inside source list internetacces_Fromdocker_cell interface Cellular0/3/0 overload
ip route 10.102.12.0 255.255.255.0 Tunnel201
ip route 10.102.22.0 255.255.255.0 Tunnel202
ip ssh bulk-mode 131072
ip ssh version 2
ip ssh pubkey-chain
  username actility
   key-hash ecdsa-sha2-nistp256 FA249B09C77A121A9759A0FC724F58A8 root@a89e080e0c1e
ip ssh server algorithm publickey ecdsa-sha2-nistp256
ip scp server enable
!
!
ip access-list extended Tunnel201
 10 permit ip host 192.168.2.9 host 10.102.12.10
ip access-list extended Tunnel202
 10 permit ip host 192.168.2.9 host 10.102.22.10
ip access-list extended internetacces_Fromdocker
 10 permit ip 192.168.2.0 0.0.0.255 host 8.8.8.8
 11 permit ip 192.168.2.0 0.0.0.255 host 52.200.161.236
ip access-list extended internetacces_Fromdocker_cell
 10 permit ip host 192.168.2.9 host 8.8.8.8
!
ip sla 1
 icmp-echo 8.8.8.8 source-interface GigabitEthernet0/0/0
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 8.8.8.8 source-interface Cellular0/3/0
ip sla schedule 2 life forever start-time now
ip access-list standard 1
 11 permit any
dialer-list 1 protocol ip permit
```

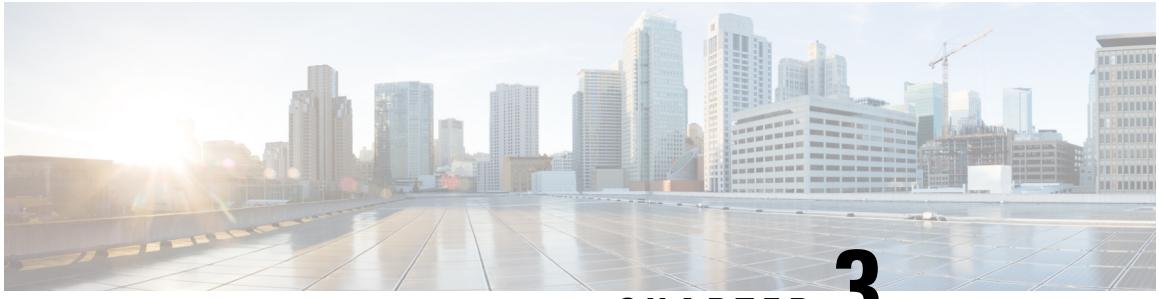
```
!
!
control-plane
!
!
line con 0
 stopbits 1
line 0/0/0
line 0/2/0
line vty 0 4
 transport input ssh
line vty 5 14
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
ntp server 0.pool.ntp.org
ntp server 1.pool.ntp.org
ntp server 2.pool.ntp.org
!
!
event manager applet restart_actility_lrr
 event none sync yes maxrun 60
 action 1 cli command "enable"
 action 2 cli command "app-hosting stop appid APFC1"
 action 3 wait 5
 action 4 cli command "app-hosting start appid APFC1"
event manager applet Cellular_Activate
 event track 1 state down
 action 1 cli command "enable"
 action 2 cli command "configure terminal"
 action 3 cli command "interface Cellular 0/3/0"
 action 4 cli command "no shut"
 action 5 cli command "end"
event manager applet Cellular_Deactivate
 event track 1 state up
 action 1 cli command "enable"
 action 2 cli command "config terminal"
 action 3 cli command "interface Cellular 0/3/0"
 action 4 cli command "shutdown"
 action 5 cli command "end"
!
end

Router#
```

Debug Commands

The following debug commands are available:

```
Router#debug lorawan ?
cli     lorawan cli trace
errors  lorawan error messages
info    lorawan info messages
Router#
```

```
Router#debug lorawan cli
cli trace debugging is on
Router#

Router#debug lorawan errors
error debugging is on
Router#

Router#debug lorawan info
info debugging is on
Router#
```



CHAPTER 3

Regulatory and Compliance Information for the LoRaWAN Pluggable Interface Module

This chapter contains the following sections:

Related Documentation

The following are the various locations containing important information:

- Cisco.com: www.cisco.com
- Warranty Information: www.cisco-warrantyfinder.com
- Cisco Information Packet, consisting of Cisco Limited Warranty, Disclaimer of Warranty, End User License Agreement, and United States Federal Communications Commission Notice: www.cisco.com/en/US/docs/general/warranty/English/SL3DEN.html
- Cisco Marketplace: www.cisco.com/pcgi-bin/marketplace/welcome.pl
- Cisco Product Documentation: www.cisco.com/go/techdocs
- Cisco Support: www.cisco.com/cisco/web/support/index.html

Installation Warning and Caution Statements

Caution Airflow around the router must be unrestricted. The dimensions (height x width x depth) are 7.70 x 11 x 1.73 in. (19.6 x 27.9 x 4.39 cm). To prevent the router from overheating, there must be a minimum of 1.0 in. (25.4 mm) around all surfaces of the router. Contact your Cisco Technical Assistance Centre (TAC) if tighter spacing is required.

Warning In order to comply with FCC radio frequency (RF) exposure limits, antennas for this product should be located a minimum of 7.9 in. (20 cm) or more from the body of all persons. **Statement 332**

Warning This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. **Statement 1017**

Warning To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 140°F (60°C). **Statement 1047**

Warning Use twisted-pair supply wires suitable for 86°F (30°C) above surrounding ambient temperature outside the enclosure. **Statement 1067**

Warning Avoid using or servicing any equipment that has outdoor connections during an electrical storm. There may be a risk of electric shock from lightning. **Statement 1088**

Caution The equipment shall only be used in an area of at least pollution degree 2 as defined by EN 60079-0. In addition, the Equipment shall be installed in a certified enclosure that provides a degree of protection not less than IP54 in accordance with EN IEC 60079-0 (for ATEX) or UL 60079-0 (for US Zones) and is accessible by a tool only.

Note This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D, or only nonhazardous locations.

Note This equipment is rated as follows- DC Input Voltage: Maximum Operating Range: 9.6V to 32VDC; Nominal: 12/24 VDC.

Note This product is suitable for use in environmental air space in accordance with Section 300.22.C of the National Electrical Code and sections 2-128, 12-010(3), and 12-100 of the Canadian Electrical Code, Part 1, C22.1. You should not install the power supply or power injector in air-handling spaces.

Note The maximum ambient operating temperature range is –40 to 140°F (–40 to 60°C).

Hazardous Locations Standards and Marking Strings

The following standards were used for the hazardous locations approvals and certifications:

- CSA C22.2 No. 60079-0:19, 4th Ed., Issued 2019-0
- CAN/CSA-C22.2 No. 60079-7:16, 2nd Ed., Issued 2016-10
- CSA C22.2 No. 213-17, 3rd Ed., Rev. 2019-08-26
- EN IEC 60079-0:2018 EN IEC 60079-7: 2015 +A1:2018
- EN IEC 60079-7: 2015 +A1:2018
- UL 121201, 9th Ed., Rev. 2019-08-26
- UL 60079-0 ,7th Ed., Rev. 2020-04-15
- UL 60079-7 5th Ed. Rev. 2017-04-21

- Class 1, Div 2, Groups A B C D
- Class I, Zone 2, AEx ec IIC T4 Gc
- DEMKO 18 ATEX 2089X
- Ex ec IIC T4 Gc

EMC Information

For EMC and safety information, see the Regulatory Compliance and Safety Information for Cisco IoT Series Routers document.

Class A Notice for FCC

Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In such an event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The Part 15 radio device operates on a noninterference basis with other devices operating at this frequency when using the integrated antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

OEM Warning statement (Module)

The modular transmitter must be equipped with either a permanently affixed label or must be capable of electronically displaying its FCC/ISED identification number:

If using a permanently affixed label, the modular transmitter must be labeled with its own FCC/ISED identification number, and, if the FCC identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: "Contains Transmitter Module FCC ID: LDKLPWA900, IC: 2461A-LPWA900." Any similar wording that expresses the same meaning may be used. The Grantee may either provide such a label, an example of which must be included in the application for equipment authorization, or, must provide adequate instructions along with the module which explain this requirement. In the latter case, a copy of these instructions must be included in the application for equipment authorization.

L'émetteur modulaire doit être équipé soit d'une étiquette apposée en permanence, soit être capable d'afficher électroniquement son numéro d'identification FCC/ISED :

Si vous utilisez une étiquette apposée de manière permanente, le transmetteur modulaire doit être étiqueté avec son propre numéro d'identification FCC/ISED et, si le numéro d'identification FCC n'est pas visible lorsque le module est installé à l'intérieur d'un autre appareil, alors l'extérieur de l'appareil dans lequel le module est installé doit également afficher une étiquette faisant référence au module fourni. Cette étiquette extérieure peut utiliser une formulation telle que : « Contient l'ID FCC du module émetteur : LDKLPWA900, IC: 2461A-LPWA900». Toute formulation similaire exprimant le même sens peut être utilisée. Le bénéficiaire peut soit fournir une telle étiquette, dont un exemple doit être inclus dans la demande d'autorisation d'équipement, soit fournir des instructions adéquates avec le module expliquant cette exigence. Dans ce dernier cas, une copie de ces instructions doit être jointe à la demande d'autorisation d'équipement.

List of Applicable FCC Rules

This module has been tested for compliance to FCC Part 15C (FCC Part 15.247).

Additional testing, Part 15 Subpart B disclaimer

This transmitter module is tested as a subsystem and its certification does not cover the FCC Part 15 Subpart B (unintentional radiator) rule requirement applicable to the final host. The final host will still need to be reassessed for compliance to this portion of rule requirements if applicable. As long as all conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

Industry Canada

Canadian Compliance Statement

Cisco® LoRaWAN Pluggable Interface Module: P-LPWA-900

Industry Canada Certification Number: 2461A-LPWA900

This Class A Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

This device complies with Class A Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco® LoRAWAN Module P-LPWA-900 is certified to the requirements of RSS-247. The use of this device in a system operating either partially or completely outdoors.

This device has been designed to operate with antennas having a maximum gain of 5.6 dBi. Antennas having a gain greater than 5.6 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotopically radiated power (EIRP) is not more than that permitted for successful communication.

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Cisco® LoRaWAN Pluggable Interface Module PIDs: P-LPWA-800

Declaration of Conformity with Regard to EU Directive 2014/53/EU

The information in this document is applicable to the Cisco LoRaWAN Pluggable Interface Module.

The P-LPWA-800 operates in the 863-870MHz frequency range in the European region.

National regulations may require operations to be limited to portions of the frequency ranges identified above or at reduced power levels, or both. See the National Restrictions section for complete details.

This declaration is only valid for configurations (combinations of software, firmware and hardware), provided or supported by Cisco Systems for use within the EU or countries that have implemented the EU directives. The use of software or firmware not supported or provided by Cisco Systems may result in the equipment not being compliant with the regulatory requirements.

Table 6: Country Statements

Country	Statement
Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 2014/53/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 2014/53/EU.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 2014/53/EU.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 2014/53/EU.
Eesti [Estonian]:	See seade vastab direktiivi 2014/53/EL olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 2014/53/UE.

Country	Statement
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 2014/53/ΕΕ.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 2014/53/UE.
Hrvatski:[Croatian]	Ova oprema je u sukladnosti s bitnim zahtjevima i drugim relevantnim odredbama Direktive 2014/53/EU
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 2014/53/EU.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 2014/53/UE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 2014/53/ES Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 2014/53/EU.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 2014/53/UE.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 2014/53/EU irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 2014/53/EU.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 2014/53/UE.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 2014/53/UE.
Română [Romanian]	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 2014/53/EU.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 2014/53/UE.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 2014/53/EÚ.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 2014/53/EU olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 2014/53/EU.

Country	Statement
Türk [Turkish]	Bu cihaz 2014/53/EU Direktifi'nin temel gereklerine ve ilgili diğer hükümlerine uygundur.

Declaration of Conformity for RF Exposure

This section contains information on compliance, with guidelines related to RF exposure.

RF Exposure

Cisco products are designed to comply with the following national and international standards on human exposure to RF:

- US 47 Code of Federal Regulations Part 2 Subpart J
- American National Standards Institute (ANSI) / Institute of Electrical and Electronic Engineers / IEEE C 95.1
- International Commission on Non Ionizing Radiation Protection (ICNIRP)
- Ministry of Health (Canada) Safety Code 6. Limits on Human Exposure to Radio Frequency Fields in the range from 3kHz to 300 GHz
- Australia Radiation Protection Standard

Note To ensure compliance with various national and international Electromagnetic Field (EMF) standards, the system should only be operated with Cisco-approved antennas and accessories.

This Device Meets International Guidelines for Exposure to Radio Waves

The LoRAWAN module P-LPWA includes a radio transmitter and receiver. It is designed to not exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) recommended by international guidelines. The guidelines were developed by an independent scientific organization (ICNIRP) and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated as to avoid contact with the antennas by the end user. We recommended that you set the system in a location where the antennas can remain at least at a minimum distance, as specified, from a user in accordance with the regulatory guidelines that are designed to reduce the overall exposure to a user or operator.

The World Health Organization has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure, then you can easily do so by reorienting antennas away from users, or by placing he antennas at a greater distance than recommended.

This Device Meets FCC Guidelines for Exposure to Radio Waves

The LoRAWAN module P-LPWA includes a radio transmitter and receiver. It is designed to not exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in FCC Part 1.1310. The guidelines are based on IEEE ANSI C 95.1 and include a substantial safety margin designed to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated so as to avoid contact with the antennas by the end user. We recommend that you set the system in a location where the antennas can remain at least at a minimum distance, as specified, from a user in accordance with the regulatory guidelines that are designed to reduce the overall exposure to a user or operator.

The device has been tested and found compliant with the applicable regulations as part of the radio certification process.

The U.S. Food and Drug Administration has stated that present scientific information does not indicate the need for any special precautions for the use of wireless devices. The FCC recommends that if you are interested in further reducing your exposure, you can easily do so by reorienting antennas away from users, or by placing the antennas at a greater distance than recommended, or by lowering the transmitter power output.

Note The RF Exposure Calculation is done without compensating cable and connector losses. The RF Exposure calculation is performed with the highest supported antenna gain.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator and your body.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Device Meets the Industry Canada Guidelines for Exposure to Radio Waves

The P-LPWA-900 is designed to not exceed the limits for exposure to radio waves (radio frequency electromagnetic fields) as referenced in Health Canada Safety Code 6. The guidelines include a substantial safety margin designed into the limit to ensure the safety of all persons, regardless of age and health.

As such the systems are designed to be operated so as to avoid contact with the antennas by the end user. We recommend that you set the system in a location where the antennas can remain at leastat a minimum distance, as specified, from a user in accordance with the regulatory guidelines that are designed to reduce the overall exposure to a user or operator.

Note Health Canada states that present scientific information does not indicate the need for any special precautions for the use of wireless devices. They recommend that if you are interested in further reducing your exposure, you can easily do so by reorienting antennas away from users by placing the antennas at a greater distance than recommended, or by lowering the transmitter power output.

ISED Radiation Exposure Statement

This equipment complies with ISED RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 36cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 36cm de distance entre la source de rayonnement et votre corps

Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

CAN ICES-3 (A)/NMB-3(A)

The Country Code Selection feature is disabled for products marketed in the US/Canada.

Additional Information on RF Exposure

You can find additional information on RF exposure in the following links:

- FCC Bulletin 56: Questions and Answers about Biological Effects and Potential Hazards of Radio Frequency Electromagnetic Fields
- FCC Bulletin 65: Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields
- FCC Bulletin 65C (01-01): Evaluating Compliance with the FCC guidelines for Human Exposure to Radio Frequency Electromagnetic Fields: Additional Information for Evaluating Compliance for Mobile and Portable Devices with FCC limits for Human Exposure to Radio Frequency Emission

You can obtain additional information from the following organizations:

- World Health Organization Internal Commission on Non-Ionizing Radiation Protection.
- United Kingdom, National Radiological Protection Board.
- Cellular Telecommunications Association.
- The Mobile Manufacturers Forum.

EMC Class A Notices and Warnings

Statement 340—Class A Warning for CISPR32

Danger Warnung	**Danger** Dies ist ein Produkt der Klasse A. Bei der Verwendung dieses Produkts im Haus- oder Wohnungsbereich kann es zu Funkstörungen kommen. In diesem Fall muss der Benutzer u. U. angemessene Maßnahmen ergreifen.

National Restrictions

The following sections identify the countries having additional requirements or restrictions.

Brazil Regulatory Information

English Translation

This equipment is not entitled to the protection from harmful interference and may not cause interference with duly authorized systems.

Portuguese Translation

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Taiwan Regulatory Information

BSMI Class A warning

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策

Korean Regulatory Information

EMC Class A

This device may have radio interference during use and may receive harmful interference from other devices.

이 기기는 사용 중 전파혼신 가능성이 있으며, 타 기기로부터 유해한 혼신을 받을 수 있음

Statement 191—Voluntary Control Council for Interference (VCCI) Class A Warning for Japan

Warning This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, you may be required to take corrective actions.

ステートメント 191—日本向け VCCI クラス A に関する警告

警告 この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き 起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求される ことがあります。

VCCI-A

Statement 1008—Class 1 Laser Product

Warning This product is a Class 1 laser product.

ステートメント 1008—クラス 1 レーザー製品

警告 クラス 1 レーザー製品です。

Statement 1051—Laser Radiation

Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

ステートメント 1051： レーザー放射

警告 接続されていない光ファイバ ケーブルやコネクタからは目に見えないレーザー光が放射されている可能性があります。レーザー光を直視したり、光学機器を使用して直接見たりしないでください。

Statement 1255—Laser Compliance Statement

Warning Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019.

聲明4011—國家通信委員會警告

警告 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Changing Output Power

Changing the power output is allowed only by a trained service professional.

Obtaining Documents from Cisco.com

Follow these steps to obtain any of the online documents mentioned in this document.

Browse to this URL on Cisco.com:
http://www.cisco.com/cisco/web/psa/default.html?mode=prod&level0=278875243

Note If you still have questions regarding the compliance of these products, or you cannot find the information you are looking for, send an email to Cisco at complianceinfo@cisco.com.